UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF MARYLAND

IN THE MATTER OF THE	*	
SEARCH OF THE PREMISES	*	15 - 362 BPG
COMMONLY KNOWN AS	*	**CRIM. NO.** _____
308 MOUNTAIN RIDGE CT, APT. J	*	
GLEN BURNIE, MARYLAND 21061	*	

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

Your Affiant, Christine D. Carlson, being duly sworn, depose and state that:

1. Your Affiant is a Special Agent (SA) with the Department of Homeland Security, Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the Special Agent in Charge in Baltimore, Maryland and has been so employed since June 1996. As part of the daily duties as an HSI agent, your Affiant investigates criminal violations relating to child exploitation and child pornography including violations pertaining to the illegal production, distribution, receipt, and possession of child pornography, in violation of Title 18, U.S.C. §§ 2251 and 2252A. Your Affiant has received training in the area of child pornography and child exploitation, and has had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. Your Affiant has also participated in the execution of search warrants that involved child exploitation and/or child pornography offenses. Your Affiant has received formal training from U.S. Customs, HSI and other agencies in the area of child pornography, pedophile behavior, collectors of other obscene material and Internet crime.

JTM
2013R02380

PURPOSE OF THIS AFFIDAVIT

2. This Affidavit is made in support of an application for a warrant to search the entire premises located at 308 Mountain Ridge Court, Apt. J, Glen Burnie, Maryland 21061 (the SUBJECT PREMISES), more specifically described in Attachment A, which is incorporated herein by reference. The purpose of this application is to seize evidence of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B) which make it crimes to distribute and possess child pornography.

3. As a federal agent, your Affiant is authorized to investigate violations of laws of the United States and is a law enforcement officer with the authority to execute warrants issued under the authority of the United States.

4. Your Affiant is familiar with the information contained in this Affidavit based upon the investigation your Affiant has conducted and based on your Affiant's conversations with other law enforcement officers who have engaged in numerous investigations involving child pornography. The information contained in this affidavit came from your Affiant's own participation in the inquiry described herein, as well as from other law enforcement officers and other third parties.

5. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, your Affiant has not included each and every fact known concerning this investigation. Your Affiant has set forth only those facts that your Affiant believes are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B) are located at the SUBJECT PREMISES.

SUMMARY

6. This investigation has revealed that an individual residing at 308 Mountain Ridge Court, Apt. J, Glen Burnie, Maryland 21061 distributed 5 video files depicting minors engaged in sexually explicit conduct.

SUMMARY CONCERNING CHILD PORNOGRAPHY, PERSONS WHO POSSESS AND COLLECT CHILD PORNOGRAPHY AND HOW USE OF COMPUTERS AND THE INTERNET RELATES TO THE POSSESSION, RECEIPT AND DISTRIBUTION OF CHILD PORNOGRAPHY

7. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I have learned that individuals who utilize the internet generally, and Peer to Peer applications specifically, to view and receive images of child pornography are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Individuals who have a sexual interest in children or images of children may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Individuals who have a sexual interest in children or images of children may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or

images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children or images of children frequently maintain their "hard copies" of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children or images of children often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector's residence, to enable the individual to view the collection, which is valued highly.

e. Individuals who have a sexual interest in children or images of children also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/collectors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone

numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who would have knowledge on how to access a Peer to Peer network to distribute and possess child pornography to others would have gained knowledge of its location through online communication with others of similar interest. Other forums, such as bulletin boards, newsgroups, IRC chat or chat rooms have forums dedicated to the trafficking of child pornography images. Individuals who utilize these types of forums are considered more advanced users and therefore more experienced in acquiring a collection of child pornography images.

g. Individuals who have a sexual interest in children or images of children prefer not to be without their child pornography for any prolonged time period. This behavior has been consistently documented by law enforcement officers involved in the investigation of child pornography.

8. In addition, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily available forensic tools.

a. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard

drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten.

b. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages.

c. The storage capacity of personal computers has increased dramatically over the last few years. Common and commercially available hard drives are now capable of storing over 500 GB of data. With that amount of storage space, an individual could store thousands of video files and/or hundreds of thousands of image files.

d. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. Since the storage capacity of hard drives has increased dramatically over the last several years, it is more likely that the above described information will be recovered during forensic analysis.

9. Based on traits shared by collectors, the ability of a forensic analyst to find data long after it has been deleted, and the increased storage capacity of computers over time, there exists a fair probability that evidence regarding the

distribution, receipt and possession of child pornography will be found at the target residence notwithstanding the passage of time. In addition, based on this target's activity, detailed below, which consisted of making at least five video files available for others to download via a peer-to-peer network there is reason to believe the target has both collected images of child pornography and distributed child pornography.

Peer to Peer (P2P)

10. Peer-to-peer (P2P) file sharing is a method of communication available to Internet users through the use of special software, which can be downloaded from the internet. Computers linked together through the internet using this software form a network that allows for the sharing of digital files between users on the network. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files that are currently being shared on the network. Some types of P2P software set up their searches by keyword. The results of the keyword search are displayed to the user. The user then selects file(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file.

11. For example, a person interested in obtaining child pornographic images would open the P2P application on his/her computer and conduct a search for files using a term such as "preteen sex." The search is sent out over the network of computers using compatible P2P software. The results of the search are returned to the user's computer and displayed. The user selects from the results displayed of the

file(s) he/she wants to download. The file is downloaded directly from the computer hosting the file. The downloaded file is stored in the area previously designated by the user. The downloaded file will remain there until moved or deleted.

12. One of the advantages of P2P file sharing is that multiple files may be downloaded at the same time.

13. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers.

14. Third party software is available to identify the IP address of the P2P computer sending the file and to identify if parts of the file came from one or more IP addresses. Such software monitors and logs Internet and local network traffic.

PROBABLE CAUSE

15. On November 19, 2014, HSI Special Agent Scott Stein used an undercover computer connected to the internet to conduct investigations into the sharing of child pornography on the eDonkey2000 (eD2k) file sharing network and its software interface named eMule. The eD2k network is one of several peer-to-peer (P2P) file sharing networks on the internet. eMule is the most popular software interface for the eD2k network and is open source software that is free for anyone to download.

16. On November 19, 2014, between 06:50:22 GMT and 11:19:38 GMT, a direct connection was established on the eD2k network with IP address 73.173.193.101. SA Stein was able to successfully download five videos that the

computer at IP address 73.173.193.101 was making available on the eD2k network. Your Affiant has reviewed all five videos downloaded from the computer at IP address 73.173.193.101 and determined that all five video files are child pornography as defined in Title 18, United States Code, Section 2256(a). Three of the five videos downloaded from IP address 73.173.193.101 are described as follows:

a. **Kidcam 2011 – Vichatter 7-10yo cute girl on webcam posing preteen slut.mpg** – this moving digital image is approximately 12 minutes and 26 seconds long and depicts a prepubescent female using a webcam. During the video, the prepubescent female pulls her pants down exposing her genitalia to the camera, then using her left hand, rubs her genitalia. The prepubescent female then uses both hands to spread the "lips" of her vagina for the camera.

b. **Girl Lolipop – Unknown – Little 6yo and dad (Hussyfan) (pthc) (r@ygold) (babyshivid).mpg** – this moving digital image is approximately 7 minutes and 44 second long and depicts a prepubescent female's mouth being penetrated by the penis of an adult male, and also depicts the adult male putting his mouth on the prepubescent female's vagina.

c. **Thai PTHC 2009 Lillipop Issue 1-04b. DEBBIE OPENS HER LITTLE BAD PUSSY..avi** – this moving digital image is approximately 6 minutes and 19 second long and depicts a naked prepubescent female lying on a bed with her legs spread. The prepubescent female rubs oil all over her body. The prepubescent female then gets on her hands and knees and exposes her genitalia to the camera. The camera zooms in on the prepubescent female's vagina.

17. On November 25, 2014, SA Stein sent a DHS summons to Comcast requesting subscriber information for IP address 73.173.193.101 from November 1, 2014 through November 25, 2014 covering the date and times the videos were downloaded.

18. On December 1, 2014, Comcast responded to the summons and identified the subscriber of IP address 73.173.193.101 beginning November 19, 2014 at 05:13:25 GMT through December 1, 2014 (the date of the summons response) as Mark

COHEN, 308 Mountain Ridge Court, Apt. J, Glen Burnie, Maryland 21061 (the SUBJECT PREMISES), telephone: 443-270-6024, account status: active.

19. On January 27, 2015, your Affiant obtained a digital photograph of Mark COHEN from the Maryland Motor Vehicle Administration records. Maryland Motor Vehicle Administration records reflect 308 Mountain Ridge Court, Apt. J, Glen Burnie, Maryland 21061, the SUBJECT PREMISES, as COHEN's current address.

20. On January 27, 2015, your Affiant obtained Maryland wage and hour records for COHEN and identified his employer as Henderson Webb, Inc. A Google search for Henderson Webb identified the company as "Your hometown property management company". One of the apartment complexes listed under Hendersen Webb's management is Mountain Ridge Apartments where COHEN resides.

21. On January 29, 2015, your Affiant conducted surveillance at the SUBJECT PREMISES and observed a blue Ford, 2-door, bearing Maryland tag 79139L and a black Dodge Charger, bearing Maryland tag 3BD1960 parked in the vicinity of the SUBJECT PREMISES which is located in the Mountain Ridge Apartment complex. Both vehicles were covered in snow and appeared not to have been driven in a few days. Your Affiant also observed a black trailer parked between the two vehicles. The trailer was bearing Maryland tag 70528TL. A check of the Maryland Motor Vehicle Administration records revealed the registered owner of the vehicles to be Mark COHEN at the SUBJECT PREMISES. These are the only two vehicles registered to COHEN. COHEN also has two motorcycles registered in his name.

22. On January 29, 2015, your Affiant sent a summons to Comcast for subscriber information using the address of the SUBJECT PREMISES. On February 3,

2015, Comcast responded to the summons identifying the subscriber as Mark COHEN and the account status as "active". Additionally, Comcast records revealed that IP 73.173.193.101, the IP that was sharing files via the eD2k P2P network on November 19, 2014, was still a current IP address at the SUBJECT PREMISES.

23. On February 19, 2015, a representative from the U.S. Postal Service informed your Affiant that Mark COHEN was receiving mail at 308 Mountain Ridge Court, Apt. J, Glen Burnie, Maryland 21061 (the SUBJECT PREMISES).

24. Your Affiant has been to 308 Mountain Ridge Court, Glen Burnie, Maryland, and observed through the glass on either side of the front entrance that it appears that there are four doors on the first floor, indicative of four apartments. In addition, there are "buzzers" for apartments "A" through "L" on the exterior of the left side of the front door as you are facing the door. In addition, there are six mailboxes on each side of the interior of the building which are visible through the glass by the front door. However, due to the entrance to building 308 being locked and the fact that it appears that the Target is associated with the management of the apartment complex, your Affiant has not been able to access the interior of 308 Mountain Ridge Court due to concerns about potentially compromising the investigation.

25. Given the foregoing information, your Affiant believes an individual located at 308 Mountain Ridge Court, Apt. J, Glen Burnie, Maryland (the SUBJECT PREMISES) is making videos depicting children engaged in sexually explicit conduct available for others to download through a peer-to-peer program via the Internet. Your Affiant submits there is probable cause, therefore, to believe evidence of violations of 18 U.S.C. Sections 2252(a)(2), and 2252(a)(4)(B) will be found at 308 Mountain Ridge

15 - 362 BPG

Court, Apt J., Glen Burnie, Maryland (the SUBJECT PREMISES), to include on any computers and storage media located within the residence.

CONCLUSION

26. Based on the above information, there is probable cause to believe that 18 U.S.C. §§ 2252(a)(2) and 2252(a)(4)(B), which, among other things, make it a federal crime for any person to distribute and possess child pornography, have been violated, and that the property, evidence, fruits and instrumentalities of these offenses listed in Attachment B, which is incorporated herein by reference, are located at the SUBJECT PREMISES.

27. Based upon the foregoing, your Affiant respectfully requests that this Court issue a search warrant for the SUBJECT PREMISES, more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B.

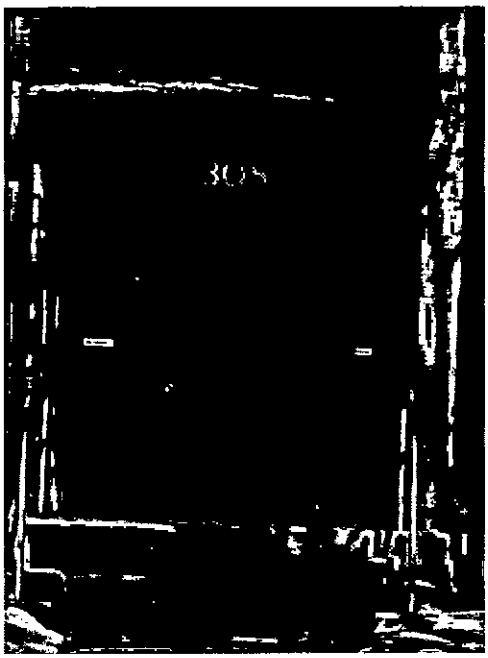
Christine D. Carlson
Special Agent
Homeland Security Investigations

Subscribed and sworn before me
this 26TH day of February, 2015

HONORABLE BETH P. GESNER
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF PROPERTY TO BE SEARCHED

308 Mountain Ridge Court, Apt. J, Glen Burnie 21061 (the SUBJECT PREMISES), which is more particularly described as a three story building located within the Mountain Ridge apartment complex. The building consists of 12 individual apartments; four apartments on each floor. The front facing of the building is brick and the numbers "308" are affixed to the glass above the brown front door. A photograph of apartment building "308" appears below.



ATTACHMENT B
DESCRIPTION OF ITEMS TO BE SEIZED

1. Computer(s), computer hardware, software, related documentation, passwords, data security devices, videotapes, video recording devices, video recording players, monitors, and or televisions, flatbed scanners, electronic devices capable of connecting to the internet or storing electronic data such as tablets, PDAs, and similar electronic devices and data that may constitute instrumentalities of, or contain evidence related to, the crimes set for in the accompanying Affidavit.

2. Any and all web cameras, cameras, film, cell phones with cameras and/or Internet capability, or other photographic equipment.

3. Any and all notes, documents, records, or correspondence pertaining to child pornography as defined under Title 18, United States Code, Section 2256(8).

4. Any and all correspondence identifying persons transmitting, receiving or possessing, through interstate commerce including by U.S. Mails or by computer, any visual depictions of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

5. Any and all records, documents, invoices and materials that concern any accounts with any Internet Service Provider.

6. Any and all visual depictions of minors.

7. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate commerce including by United States Mails or by computer, and visual depiction of minors engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

8. Any and all address books, names, and lists of names and addresses of minors visually depicted while engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

9. Any and all documents, records, or correspondence pertaining to occupancy at 308 Mountain Ridge Court, Apt. J, Glen Burnie, Maryland 21061.

10. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while

engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(2).

11. Any and all records relating to persuading, inducing, enticing or coercing any minor to engage in any sexual activity in violation of the law.

As used above, the terms "records, documents, messages, correspondence, data, and materials" includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.

12. For any computer, computer hard drive, or other physical object upon which computer data can be recorded including but not limited to tablets, PDAs, and other electronic devices (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

i. contextual information necessary to understand the evidence described in this attachment.

13. Any of the items described in paragraphs 1 through 12 above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer related equipment, including floppy diskettes, fixed hard disks, or removable hard disk cartridges, software or memory in any form. The search procedure of the electronic data contained in computer operating software or memory devices shall include the following techniques which shall be used to minimize the risk that those conducting the search will view information not within the scope of the warrant:

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possible recover recently deleted files;

d. "scanning" storage areas for deliberately hidden files; or

e. performing key word or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

14. If after performing these procedures, the directories, files or storage areas do not reveal evidence of fraud or financial crimes and items that related to or constitute evidence, fruits, or instrumentalities of violations of 18 USC Sections 2252(a)(2) and 2252(a)(4)(B), the further search of that particular directory, file or storage area, shall cease.